

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF NORTH CAROLINA
STATESVILLE DIVISION

UNITED STATES OF AMERICA)	Case No. 5:16-cr-29-KDB-DCK
)	
v.)	GOVERNMENT’S SENTENCING
)	MEMORANDUM
)	
ALEKSANDR MUSIENKO)	
)	

NOW COMES the United States of America, by and through R. Andrew Murray, United States Attorney for the Western District of North Carolina, and hereby submits this sentencing memorandum.

I. FACTUAL BACKGROUND

Defendant Aleksandr Musienko partnered with Eastern European computer hackers to obtain almost \$3 million from U.S. victims’ bank accounts and launder the stolen funds from U.S. bank accounts overseas over a three-year period. Musienko’s cybercriminal partners completed “Bank Account Takeover” schemes in which they hacked and stole information from victims in the United States and used that information to impersonate the victims. By tricking the victims’ banks into believing that withdrawals from the victims’ accounts were actually requested by the victims, the cybercriminals were able to steal large amounts of money from the victims’ accounts.

Musienko’s role involved recruiting, supervising, and directing a network of “money mules” with American corporate and individual bank accounts that could receive the stolen funds and transmit it overseas. Musienko, under the alias Robert Davis, recruited American mules by advertising on employment websites that he was hiring a financial assistant for two fake front companies under his control. Musienko instructed the mules, who believed they were working for a legitimate business, that they were to assist clients transfer funds overseas by receiving the funds

in their own bank accounts then wiring it directly to overseas accounts or via Western Union to overseas individuals. Musienko gave the mules specific instructions regarding the dollar amounts, account numbers, and recipients of the overseas transfers. Musienko took approximately 25% of the stolen funds as his fee and allowed the money mules to retain approximately 5% of their overseas wires as payment. From about October 2009 through in or about March 2012, Musienko's criminal money mule services resulted in the theft and laundering of at least \$5 million.

In September 2011, Musienko's cybercriminal partners used malware to remotely hack the computer of the Chief Financial Officer of Von Drehle Corporation and stole the log-in credentials for Von Drehle's bank account. The cybercriminals transferred a total of \$296,278.00 from Von Drehle's bank account to two bank accounts controlled by Musienko's mules. Musienko instructed the mules to wire the funds to several European bank accounts, although Von Drehle's bank detected the fraud and deducted \$197,526.36 in stolen funds from one of the mules before it was wired overseas.

In or about April 2019, the Federal Bureau of Investigation ("FBI") searched a laptop owned and controlled exclusively by Musienko. On the laptop, the FBI identified files containing approximately 120,000 payment card numbers and associated identifying information for persons other than Musienko. Musienko did not legally obtain the payment card numbers and associated information. Musienko obtained the payment card numbers and associated information in or about 2018, and did not use the information during the offense of conviction, in preparation for that offense, or in the course of attempting to avoid detection or responsibility for that offense.

II. PROCEDURAL HISTORY

On June 21, 2016, Defendant Aleksandr Musienko was charged in a sealed indictment with wire fraud, bank fraud, conspiracy to commit money laundering, and money laundering. Musienko

was arrested in South Korea in 2018 and extradited to the United States, and he made his initial appearance in this district on March 29, 2019. On November 20, 2019, Musienko pleaded guilty to one count of wire fraud in violation of 18 U.S.C. §§ 1343 and 3559(g)(1). The Plea Agreement (Doc. 31) and Factual Basis (Doc. 30) were fully incorporated into the Presentence Report and contain a recitation of the facts of the case. (Doc. 38 ¶¶ 5-29.) The United States did not submit a Relevant Conduct statement because the Factual Basis contained a full recitation of the facts in the case.

III. ADVISORY GUIDELINES

The PSR adopted the total offense level computation of 35, as agreed upon in the plea agreement:

Base Offense Level	USSG § 2B1.1(a)(1)	7
Specific Offense Characteristics:		
Loss Exceeded \$3.5 Million	USSG § 2B1.1(b)(1)(J)	+18
10 or More Victims	USSG § 2B1.1(b)(2)(A)(i)	+2
Sophisticated Means/Outside the United States	USSG § 2B1.1(b)(10)	+2
Unauthorized Use of Any Means of Identification	USSG § 2B1.1(b)(11)(C)(i)	+2
Manager or Supervisor	USSG § 3B1.1(c)	+2
False Registration of Domain Name	USSG § 3C1.4	+2
Total		35

(See *id.* at ¶¶ 38-46.) After a three level reduction pursuant to USSG §§ 3E1.1(a) and (b), the total offense level is 32. (*Id.* at ¶¶ 47-48.) The defendant's criminal history category is I, resulting in an advisory sentencing guideline range of 121 to 151 months. (*Id.* at ¶¶ 55, 72.) If the Court grants the Government's motion for a 3-level downward departure, the applicable guideline range will be 87 to 108 months (approximately 30% below the current guideline).

IV. 18 USC § 3553(a) SENTENCING FACTORS

The Court must consider the § 3553(a) factors in fashioning a sentence that is sufficient, but not greater than necessary, to achieve the goals of sentencing. The Court must also avoid unwarranted sentencing disparities. In particular, the nature and circumstances of the offense, history and characteristics of the defendant, the need to promote respect for the law, to afford adequate deterrence, both specific and general, and to protect the public from further crimes of the defendant support a sentence of 87 months.

A. Nature and Circumstances of the Offense.

Complex cybercrimes, particularly those involving the degree of hacking, laundering, and obfuscation present here, are some of the most serious and technically difficult crimes to defend against, identify, and investigate. Businesses must remain vigilant against an ever-growing number of possible attacks, and investigators are often required to conduct detailed forensic analyses to evaluate the scope of the intrusion and locate evidence that may eventually lead to the identity of the actors. While Musienko did not commit the intrusions at issue here, his involvement remained integral to the success of this cybercrime scheme. Stealing funds from an American bank account is usually worthless to the hacker without an effective money mule network to receive and transfer the funds out of the country. Indeed, the back-end money launderers are pivotal to the success of the hacking schemes. Even before launching attacks on U.S. victim's bank accounts, hackers line up their trusted money laundering partners to ensure the swift and successful transfer of the stolen funds. Savvy intermediaries like Musienko who can both effectively scheme with foreign cybercriminals and also convince English-speaking American mules to unwittingly participate in the scheme are as rare as they are invaluable.

Operating the scheme involved a significant amount of preparation and continuous effort.

Musienko had to keep the ruse going to prevent his mules from becoming suspicious, and he created multiple fake front businesses, aliases, domain names, email addresses, and fake job postings to lure and lull them. The sophistication involved in Musienko's front companies and mule management further shows the seriousness of the offense.

While the direct losses suffered by Von Drehle Corporation as a result of the scheme were relatively minor for a corporation of its size, the company still suffered unquantifiable business disruptions. The company was required to expend significant resources forensically investigating and remedying the intrusion, pulling employees and resources from their ordinary functions. The unknown victims of the hacks constituting the remainder of the loss attributable to Musienko suffered similar direct losses and business disruptions.

Each of these considerations demonstrates that an 87-month sentence is sufficient to reflect the seriousness of the offense.

B. History and Characteristics of the Defendant.

The PSR suggests that Musienko has been engaged in cybercrime for nearly his entire adult life. Musienko graduated from university in 2004, obtained advanced degrees in 2005 and 2008, and by his own admission, began the fraud scheme at issue in 2009, at age 26. (*See* Doc. 38 ¶¶ 59, 64, 67.) He directed it for nearly ten years until his arrest in 2018. (*Id.* at ¶ 67.) While he claims to make approximately \$2,000 per month in income from his sole proprietorship, the evidence suggests that he would have received significantly more income from his 25% share of the stolen proceeds attributable to him. Moreover, Musienko's sophistication as a cybercriminal is further demonstrated by his use of several front companies, domains, and email addresses to further the scheme; his obfuscation of his true identity; and his use of cybercrime forums in which he advertised his package of money mule services to other cybercriminals. Musienko's possession of

120,000 stolen payment cards at the time of arrest, while not directly related to the fraud scheme at issue, further demonstrates that the cybercrimes at issue here were not aberrant conduct. The Government believes that the three-year scheme charged in the Indictment and the \$3.5 million in loss attributed to Musienko may well be merely the tip of the iceberg for Musienko's history of cybercrime, and an 87-month sentence is appropriate to reflect his history and characteristics.

C. Affording Adequate Specific and General Deterrence and Protecting the Public from Further Crimes of the Defendant.

General deterrence is particularly important in this case. Cybercriminals often operate in near-complete anonymity, and the difficulties inherent in the extradition process often allows cybercriminals engaged in complex fraud schemes to feel insulated from prosecution. Sentencing Musienko to 87 months is sufficient to send the message that cybercriminals targeting American victims will be investigated and punished, providing some measure of general deterrence to similar actors.

Upon his release from imprisonment, Musienko will be deported to Ukraine. An 87-month sentence is sufficient to ensure that the public is protected from further crimes by Musienko during his imprisonment and rehabilitation.

V. RESTITUTION

The defendant has agreed, pursuant to 18 USC § 3663A, to pay restitution to the victim. (Doc. 31, Plea Agreement ¶ 9). Restitution in the total amount of \$296,278.00 is owed to Von Drehle Corporation, as set forth in the PSR. (Doc. 38 ¶ 82.)

VI. CONCLUSION

For the foregoing reasons, the United States recommends a sentence of 87 months and an order directing restitution to Von Drehle Corporation in the amount of \$296,278.00. Such a sentence reflects the seriousness of the offense and affords adequate specific and general

deterrence to future criminal conduct.

Respectfully submitted on February 1, 2021.

R. ANDREW MURRAY
UNITED STATES ATTORNEY

/s/ Graham R. Billings

Graham R. Billings
Assistant United States Attorney
NC Bar No. 55972
United States Attorney's Office
227 West Trade Street, Suite 1650
Charlotte, North Carolina 28202
Telephone: (704) 338-3137
Facsimile: (704) 344-6629
E-mail: graham.billings@usdoj.gov

/s/ Mona Sedky

Mona Sedky
Senior Trial Attorney
U.S. Dept. of Justice, Criminal Division
Computer Crime & Intellectual Property Section
1301 New York Avenue, Suite 600
Washington, DC 20580
Telephone: (202) 353-4304
Facsimile: (202) 514-6113
E-mail: mona.sedky@usdoj.gov